Multinational Experiment 7
Outcome 3 – Cyber Domain
Objective 3.3

Concept Framework

Version 3.0

03 October 2012

Distribution Statement

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
08 JUL 2013	**N/A**	

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Multinational Experiment 7 Outcome 3 - Cyber Domain Objective 3.3 Concept Framework Version 3.0 03 October 2012	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **JOINT STAFF-MN//ACT Integration 116 Lakeview Parkway Suffolk, VA 23435**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release, distribution unlimited.

13. SUPPLEMENTARY NOTES
The original document contains color images.

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**UU**	**17**	

Table of contents

This document was prepared by obj.3.3 legal working group, led by the following team: Prof. Talitha Vassalli di Dachenhausen of the Naples University "Federico II", RADM (ret) Pio Forlani, Dr. Rita Mazza, Dr. Annachiara Rotondo, Dr. Claudia Pirillo, and supported by IAI (Istituto Affari Internazionali / International Affairs Institute). Life Management and Configuration Control over this document, generated by the cooperative effort under MNE 7 umbrella, will be established by the Italian Defence General Staff-Centre for Defence Innovation.

FOREWORD

Multinational Experiment 7 (MNE 7) is a two-year multinational and interagency Concept Development and Experimentation (CD&E) effort aimed to improve coalition capabilities to ensure access to and use of the global commons domains (air, maritime, space and cyber) through application of the comprehensive approach.

AIM and SCOPE

Cyberspace, as defined as the virtual domain characterized by the use of electronics and the electromagnetic spectrum to store, edit and share information through computer networks and their physical infrastructure, is now an integral part of modern life. It can be seen as the immaterial dimension that connects computers around the world in a single network that allows users to interact with each other. It can also be seen as the "conceptual space" where people interact using communication technologies mediated by a computer (i.e. computer mediated communication, CMC). Cyberspace is now commonly used to refer to the "Internet world" in general.

People around the world interact, cooperate and compete through a series of networked linkages that span the globe. By a combination of simple web-based communications and more complex infrastructure networks, the cyber common enables private and public institutions to provide essential services such as energy. Banks and asset traders use internet to shift billions of dollars within seconds. Modern militaries employ cyber commons as a key enable of military operations, using commercial and private networks to support everything from command and control to logistics.

The international community has a limited ability to govern the cyber common, depending not only on the private ownership and/or control of infrastructures, but also on their location everywhere, in national and international spaces.

International law rules can provide a useful framework for the purposes of MNE 7 solution development and experimentation in order to give some parameters for Decision's Makers actions.

The MNE7 problem statement leads to a comprehensive approach. It was thus considered from a strategy perspective, namely ends, ways and means (the central triangle) and then viewed through four study areas (international norms and legal frameworks; threat assessment and vulnerability analysis; situational awareness and information sharing; and inter-domain concepts and planning constructs), and across the interdependent domains that comprise the global commons (Maritime, Air, Space, and Cyberspace) (see Figure 1).

In particular, as major project outputs, Decision Makers will be provided with tools capable to perform sufficient understanding and situational awareness of their own networks and relevant parts of wider cyberspace, in order to ensure access to and freedom of action within the cyber common. Access to, and freedom of action within, the cyber common is essential for national and international security because critical networks and infrastructures are becoming increasingly dependent upon it. Decision Makers can gain sufficient understanding (including legal understanding) and situational awareness of their own networks and relevant parts of wider cyberspace, drawing upon integrated and collaborative information, which in turn improves their ability to make timely, informed and effective decisions on the actions that allow us to anticipate, deter, prevent, protect, respond, and rapidly affect an adversary's ability to disrupt or degrade our access to, and freedom of action within, the global commons. To do so the Decision Maker should be able to identify, analyze and assess threats and vulnerabilities that may pose a risk to national and international security (e.g. to critical networks and infrastructures) by disrupting or degrading access to or freedom of action within the cyber common, as well as through hidden intrusions aimed at distorting and/or forging the data exchanged within the systems (so called man-in-the-middle – MITM - attacks).

In such a context, the aim of MNE7 objective 3.3 is to improve partners and coalition members understanding of the current legal framework applicable to the cyber common, in order to handle cyber incidents, while providing Decision Makers with the appropriate tools that support decision options for response. At this first step, objective 3.3 produced an overarching Concept Framework that outlines the main international law rules applicable to the cyber common. The purpose of the Concept Framework is to deliver a tool to participating nations that will enable them to achieve an improved understanding of the current legal

frameworks applicable to the cyber common, in order to assess, handle and make the appropriate response to emerging cyber incidents in accordance with the provisions of the current international law.

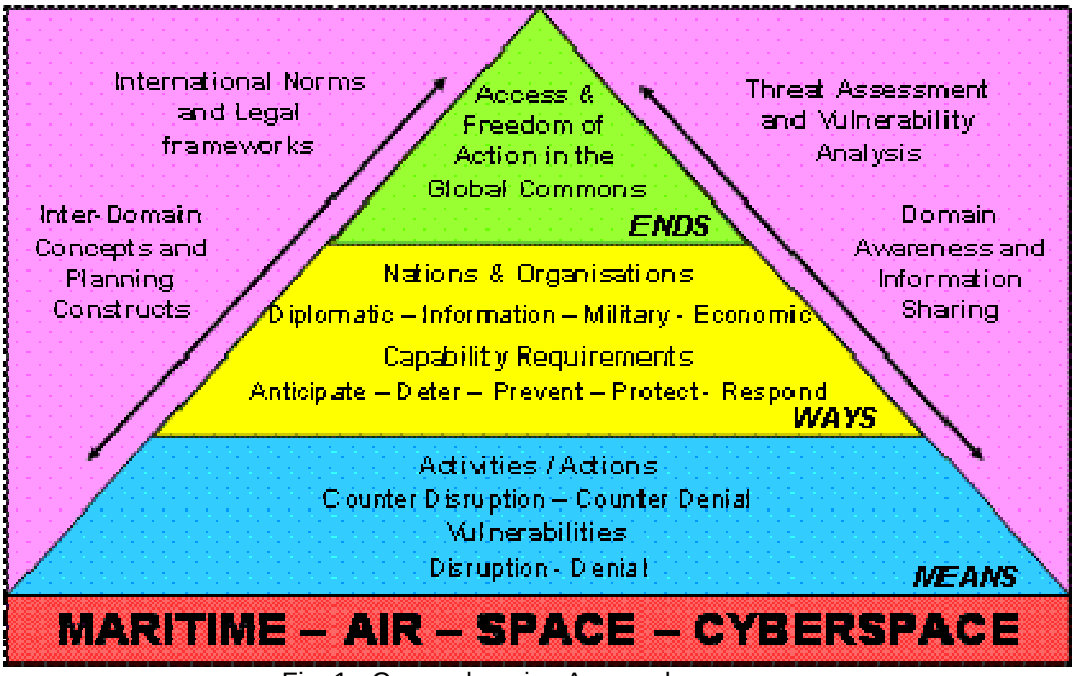

Fig. 1 =Comprehensive Approach=

A. THE CONTEXT

A.1 UBIQUITOUS (TERRITORIALITY AND JURISDICTION) -

Near other cyberspace characters, such as “speedy”, “non-coercibility”, “anonymity” and “borderless”, the ubiquity (that is, being everywhere) of cyberspace decisively characterizes it and appears to put under discussion a fundamental facet of International Law, that is: State Sovereignty.
For the purposes of MNE7, cyberspace is considered as a global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the internet, telecommunications networks, computer systems, and embedded processors and controllers. Under the International Law perspective, it is preferable to replace “common” with “domain” within the definition of “cyberspace”, since the word “common”, differently from “domain”, underlines the general and free use of a space and is employed in many definitions of cyberspace issued by scholars and international organizations. The term “cyberspace” emphasizes that it can be managed as a place.

A.2 ACTORS: MAIN STAKEHOLDERS

According to the United Nations Institute of Training and Research (UNITAR), the cyberspace involves three distinct categories of actors: **‘governments/international(or regional) organizations’**, **‘private sector’** and **‘civil society’**. Indeed, each one has an interest in everything that relates to cyberspace and, for different reasons, is an **essential stakeholder** in every attempt to codify national or international laws and/or to implement measures in this field. Governments have the power to legislate and to enforce laws. The private sector is the engine of all research and development in the sector of Information Communication Technologies (ICTs), knows the very details of the hardware and software on which its architecture is based, is the owner and/or main operator and/or administrator of critical infrastructures and plays an important role in preparing, enforcing and advising on cyber-related procedures and protocols. Finally, the civil society is the ultimate end user; benefits or suffers from its use and misuse and is quantitatively the most affected by cyber threats, but, of course, the State also has these characteristics being a relevant end user itself.
It is also possible to group these actors in two main categories, namely **‘public’** and **‘private’**. The former includes all forms of ‘public actors’ at every level (e.g. agencies, governments, international/regional organisations, international/regional agencies/bodies). Alternatively, the latter includes all kinds of ‘private actors’, which are directly or indirectly involved in the cyberspace (e.g. industries, companies, experts, technicians, academy, associations and ‘alliances’ etc.).

Furthermore, it is possible to consider a third category**, 'public/private',** which includes frameworks of cooperation between both sides at different levels at the same time and still within the above mentioned categories. A further distinction can be made between **'civilian'** and **'military'** actors, since in cyberspace the boundaries between both are blurring for different reasons (e.g. cyber threats affect both military and civilian infrastructures, the existence of dual-use technologies, some competencies related to cyber attacks fall in the responsibility of civilian security organisms, the "militarisation" of cyberspace etc.).

A.3 RESPONSIBILTY/LIABILITY

The term Responsibility refers to a general obligation to do or to abstain from something, the term Liability shows the effects of a behavior.

The notion of responsibility is close to that of "duty", whereas the notion of liability is closer to that of "risk".

Responsibility can be assumed. Liability is assigned.

The terms of responsibility and liability are both present in international law as well as in domestic law. According to International Law Commission Draft Articles on State's Responsibility, "Every internationally wrongful act of a State entails the international responsibility of that State". (With regard to "internationally wrongful act" see B.2.1)

According to the Report of the International Law Commission on the work of its forty-fourth session, 1992, No. 10, A/40/10: "...any regime of liability should be flexible enough to take account of factors such as reasonableness, due diligence, the balance of interests, equity and the need not to hinder scientific progress or economic development. At the same time, any system of liability should provide for compensation for innocent victims. Any liability regime should also take account of external intervening factors, such as acts of sabotage and war, where liability was normally shifted from the operator or the State to those responsible for the act concerned".

A.4 LAW ENFORCEMENT IS NOT EASY

The above statement underlines a general feature of international law: namely the decentralization of law enforcement. With the exception of the UN collective security system acting against violations by States of the prohibition of use of force, the implementation of responsibility of a State is entrusted to the same injured State (see art 42 International Law Commission Draft Articles on State's Responsibility). Meaningful in this perspective is the fact that, unlike domestic law, the injured State is entitled to resort to countermeasures (see Chapter 2 International Law Commission Draft Articles on State's Responsibility). In view of the difficulties to ascertain elements of features of cyber activity (see A.1), law enforcement in the matter is even less easy.

Nevertheless, international law can provide a useful framework for the purposes of MNE 7 solution development and experimentation in order to give some parameters for Decision Makers' actions.

A.5 DIFFERENT LEGAL FRAMEWORKS

The juridical framework to which we refer, in our effort to provide rules for cyberspace, is given by:

1. International Law (customary law, treaty law, law of armed conflicts);
2. International Organizations rules (hard law and soft law);
3. Private international law treaties;
4. Domestic law (out of the scope of Obj. 3.3, which takes into account only international law).

B. THE PROBLEM

B.1 HOW CAN WE USE TERRITORIALITY AND JURISDICTION CONCEPTS WITHIN CYBER COMMON?

The concept of sovereignty is the fundamental basis of the international order reaffirmed in the United Nations Charter.

State's sovereignty is territorial sovereignty, i.e., it is essentially linked to the territory and to the borders delimiting the territorial space in which States exercise sovereign functions.

The concept of sovereignty can be referred to cyberspace under two angles: the **territorial sovereignty (or territoriality)** and the **functional sovereignty**.

According to the first approach suggested and deepened by CCD COE: "a State's territorial sovereignty in cyberspace ... is the ability to exercise some measure of control over its cyberspace. Therefore it is primarily up to each State to define the exact meaning of cyber sovereignty for its purposes. Cyberspace as such cannot be reigned by any one State. Nevertheless any State can exercise control over such cyber infrastructure and activities on the territory in which it has sovereignty...."

According to the second approach, based on the functional concept of sovereignty, the object of a State's power are the activities within its territory, which come into consideration as the sphere where these activities take place. The link between activities and State is even more significant when the activities take place into global commons. Therefore, this theory can provide a useful basis to regulation of cyber activities, in view of the difficulty of their location. In other words, since cyber space is characterized by ubiquity, speed and "non-coercibility" of the activities carried out therein, the functional sovereignty can cover this intangible space just because it is linked to those activities regardless of the territory. In this perspective, the identification of those subjects performing activities in cyberspace is fundamental.

B.2 WHAT ARE THE GREY AREAS WITHIN LEGAL ASSESSMENT THRESHOLDS?

B.2.1. INTERNATIONAL LAW RULES APPLICABLE TO CYBER ATTACK

The first grey area within the legal assessment thresholds (that is, wrongful acts, international crimes (as terrorism, aggression) and armed attack (see C.1 Analytical Model, last column)), concerns the identification of international law rules, applicable to cyberspace, and linked to those thresholds. According to art 2.b (Elements of an Internationally Wrongful Act of a State) of the International Law Commission (ILC) Articles on State's Responsibility "there is an internationally wrongful act of a State when conduct consisting of an action or omission [...] (b) constitutes a breach of an international obligation of the State".
International law rules belonging to customary law applicable to cyberspace can be:

- PRINCIPLE OF NON-INTERFERENCE IN INTERNAL AFFAIRS OF STATE

From the nature of the sovereignty of States and as corollary of independence and equality of States follows that a State is prohibited to intervene in the domestic affairs of another State. This principle, to be intended as respect of domestic jurisdiction, is stated also in art.2.7 of the United Nations Charter. Referring to cyberspace, the intervention through mere intrusion by communication or hostile propaganda against foreign State, especially through incitement to revolt of its population via internet, might violate the duty of non-interference. International responsibility for these acts can be engaged if they are directly or indirectly attributable to the State. On the attribution problem see B2.2 .
Whether espionage, and consequently cyber espionage, violates the principle of non -interference or whether it is only an unfriendly act is still a matter of some debate.

- PROHIBITION OF THE USE OF FORCE AND TREATH

Prohibition of the use of force by States, that was established by art 2.4 of the United Nations Charter, has become a peremptory principle of international law (*jus cogens*). Military force may only be applied by the UN Security Council in response to threat to peace, breach of peace or acts of aggression, or by States as self defence, according to Art. 51 of UN Charter, which recognizes "the inherent right of individual or collective self-defence if an armed attack occurs". When articles 2(4) and 51 are considered together, the most evident problem is whether the scope of "use of force" in art. 2(4) coincides with that of "armed attack" in art. 51. Although there is significant debate about the scope of the self-defence right to resort to military force, it is generally agreed that art. 51 carves out an exception to art. 2(4)'s strict prohibition of force and it is widely understood that "armed attack" is, although closely related, a narrower category than "threat or use of force.
The dominant view in the United States and among its major allies has long been that the Article 2(4) "prohibition of force" and the complementary Article 51 "right of self-defence" apply to military attacks or armed violence. As noted, "term *force* as used in Article 2(4) is according to the correct and prevailing view, limited to armed force".
The plain meaning of the text supports this view, as do other structural aspects of the U.N. Charter. For example, the Charter's preamble sets out the goal that "*armed* force . . . not be used save in the common interest." Similarly, Articles 41 and 42 authorize, respectively, the Security Council to take actions not involving armed force and, should those measures be inadequate, to escalate to armed force.
However, there are textual counter-arguments, such as that Article 51's more specific limit to "armed attacks" suggests that drafters envisioned prohibited "force" as a broader category not limited to particular methods.
The existence of a loophole between art. 2(4) and 51 of the UN Charter is confirmed by art. 3 of the GA Resolution no.3314/74 (XXIX) on the definition of aggression (which is now the content of art. 8 bis par. 2 of Rome Statute of the ICC according to the resolution RC/RES.6 , 11 June 2010) trying to link art.2(4), and art.51 of the UN Chart.
On the one hand, the resolution confirms the will to consider as aggression just the "armed force", excluding all the situations related to economic or political attacks; on the other hand, the resolution clarifies that the only aggression justifying self-defence is the armed one.

However, the list provided by art 3 shows the characteristics common to all the types of aggression which is a use of force "on a relatively large scale and with substantial effects"; this feature begs for the conclusion that the scope of "armed attack" doesn't exactly correspond to that of "use of force".
Although the provisions of the resolutions are not binding as UN GA resolution, its ability to strengthen the argument that there is a gap between art 2(4) and art 51 is also reflected by the ICJ judgment in Nicaragua case (ICJ, 1986).
In *Nicaragua* case, the ICJ, also failing to define "armed attack", expressly affirmed that the use of force could be divided into two categories, "most grave" (those constituting armed attacks) and "less grave", giving the word "force" at art 2 (4) a broader meaning than art. 51.
No matter what their purpose (see below B22i), cyber attacks may represent a threat to international peace and security and should be dealt with like other recognized transnational threats. Many UN declarations about international crime also support recognizing the duty to prevent cyber attacks: these declarations urge States to take affirmative steps to prevent non-State actors from using their territory to commit acts that cause civil strife in another State. Furthermore, these declarations also support the duty of States to cooperate with one another to eliminate transnational crime, which lends credence to the duty to cooperate with victim-States during the criminal investigation and prosecution of cyber attacks. Focusing specifically on cyber attacks, States have made unilateral declarations, as well as using the UN General Assembly to make declarations about the importance of preventing cyber attacks. For instance, the UN General Assembly has called on States to criminalize cyber attacks and to deny their territory from being used as a safe haven to conduct cyber attacks through State practice. The General Assembly has also called on States to cooperate with each other during the investigation and prosecution of international cyber attacks. Furthermore, States are starting to recognize the threat that cyber attacks pose to international peace and security, with some States and the General Assembly directly recognizing cyber attacks as a danger to international peace and security. These declarations all evidence recognition that States have a duty to prevent cyber attacks as a matter of law, to include the lesser duties of passing stringent criminal laws, vigorously investigating cyber attacks, prosecuting attackers, and having the host-States cooperate with victim-States during the investigation and prosecution of cases.

- **PEACEFUL SETTLEMENT OF DISPUTES**
The United Nations Charter (art. 2.3) requires "all Members of the Organization to settle their international disputes by peaceful means in such a manner that international peace and security are not endangered". States can settle their disputes through "negotiation, enquiry, mediation, conciliation, arbitration, judicial settlement, resort to regional agencies or arrangements, or other peaceful means of their own choice" (art. 33.1 UN Charter).

- **FREEDOM OF OPINION AND EXPRESSION**
The art. 19 of United Nations International Covenant on Civil and Political Rights (1966) establishes the freedom of opinion and expression as follows "1. Everyone shall have the right to hold opinions without interference. 2. Everyone shall have the right to freedom of expression; this right shall include freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media of his choice. 3. The exercise of the rights provided for in paragraph 2 of this article carries with it special duties and responsibilities. It may therefore be subject to certain restrictions, but these shall only be such as are provided by law and are necessary: (a) For respect of the rights or reputations of others; (b) For the protection of national security or of public order (order public), or of public health or morals".

- LAW OF ARMED CONFLICTS
In the current academic discussion concerning computer network attacks the applicability of the general fundamental principles of the law of armed conflict, namely the principles of necessity, humanity, distinction and proportionality is hardly questioned.

- TREATIES
Terrorism is the so called "treaty crime" as it is regulated by international conventions and it is not taken into consideration in the Rome Statute on the International Criminal Court. There is no universally accepted definition of terrorism and cyber terrorism but only sectorial treaties on terrorism upon which member States of United Nations have agreed i.e. the Warsaw Convention on the Prevention of Terrorism, Council of Europe 16 May 2005 and the 1997 International Convention for the Suppression of Terrorist Bombing . For a wide definition of terrorism, see UNSCR 1566, 8 Oct 2004, according to which terrorism means "criminal acts, including against civilians, committed with the intent to cause death or serious bodily injury, or taking of

hostages, with the purpose to provoke a state of terror, or compel a government or international organization to do or to abstain from doing any act which contravened terrorism related conventions and protocols, were not justifiable for any reason-whether of a political, philosophical, ideological, racial, ethnic or religious nature".

On the other hand, there is actually no international legal instrument which deals specifically with "cyber terrorism".

Some authors define cyber terrorism as the convergence of terrorism and cyberspace. *"It is generally understood to mean unlawful attacks and threats of attack against computers, networks, and the information stored therein when done to intimidate or coerce a government or its people in furtherance of political or social objectives. Further, to qualify as cyber terrorism, an attack should result in violence against persons or property, or at least cause enough harm to generate fear".*

Although physical forms of cyber terrorism and cyber crime often sound very much alike, cyber crime is a crime committed through the use of information technology.

For instance; if a person hacks someone's banking account and/or steals credit card information, then it is called as cyber crime, because the attacker's intention is neither political nor social. If the same attack is directed to substantial number of banking accounts and the attacker declares that he is going to continue attacks until the government accepts his demands; moreover as a consequence of this attack people begin to fear and withdraw their money from the banks then it is labeled as cyber terrorism.

On the light of the above, cyber terrorism can be considered as the premeditated use of disruptive activities, or the threat thereof, in cyber space), with the intention to further social, ideological, religious, political or similar objectives, or to intimidate any person (including a human being, a corporate entity, a State, or a collection thereof) in furtherance of such objectives.

If, on the one hand, the US Federal Government, the FBI describes cyber-terrorism as: "a criminal act perpetrated by the use of computers and telecommunications capabilities, resulting in violence, destruction and/or disruption of services to create fear by causing confusion and uncertainty within a given population, with the goal of influencing a government or population to conform to a particular political, social, or ideological agenda.", on the other hand the Council of Europe set its focus area on cyber terrorism and the subject of CODEXTER (the Committee of Expert against Terrorism) is about cyber terrorism. It has been surveying the situation in member states to evaluate whether existing international instrument are sufficient to respond cyber threat or not.[27] The CODEXTER has concluded at the end of these meetings that the use of Internet for terrorist purposes includes several elements:

(i). attacks via the Internet that cause damage not only to essential electronic communication systems and IT infrastructure, but also to other infrastructures, systems, and legal interests, including human life

(ii). dissemination of illegal content, including threatening terrorist attacks; inciting, advertising, and glorifying terrorism; fundraising for and financing of terrorism; training for terrorism; recruiting for terrorism; as well as

(iii).other logistical uses of IT systems by terrorists, such as internal communication, information acquisition and target analysis.

-THE GENERAL PRINCIPLES OF LAW COMMON TO CIVILIZED NATIONS

The general principles of law common to civilized nations (Art. 38, par. 1 c, International Court of Justice Statute) might support recognition of a duty to prevent cyber attacks. It is a well-established principle under the domestic laws of most States that individuals should be responsible for acts or omissions that have a causal link to harm suffered by another individual. While international law is not obligated to follow the domestic laws of States, international law may be derived from the general principles common to the major legal systems of the world. Most States use causation as a principle for establishing individual responsibility, lending credence to the idea that a State's responsibility should also be based on causation. Thus, if a State failed to pass stringent criminal laws, did not investigate international cyber attacks, or did not prosecute attackers, it should be held responsible for international cyber attacks against another State because its omission helped create a safe haven for attackers to attack other States. A State's duty to prevent cyber attacks should not be based on a State's knowledge of a particular cyber attack before it occurs, but rather on its actions to prevent cyber attacks in general. Cyber attacks are extremely difficult for States to detect prior to the commission of a specific attack, and are often committed by individuals or groups who are not even on a State's radar. However, just because cyber attacks are difficult to prevent does not mean that States can breach their duty to prevent them. Stringent criminal laws and vigorous law enforcement will deter cyber attacks. States that do not enact such laws fail to live up to their duty to prevent cyber attacks.

Likewise, even when a State has stringent criminal laws, if it looks the other way when cyber attacks are conducted against rival States, it effectively breaches its duty to prevent them through its unwillingness to do anything to stop them, just as if it had approved the attacks. In other words, a State's passiveness and indifference toward cyber attacks make it a sanctuary State, from where attackers can safely operate. When viewed in this light, a State can be held indirectly responsible for cyber attacks.

B.2.2. CYBER ATTACK AND ITS ATTRIBUTION

i) The definition of cyber attack remains inconsistent. Some commentators use the term to encompass a wide variety of acts of cyber terrorism and cyber warfare and other commentators use cyber attacks as a separate category.

There have been two particularly prominent government-led efforts to understand the scope of the threat posed by cyber-attacks, one by the U.S. government and the other by the Russia- and China-led Shanghai Cooperation Organization.

The U.S. National Research Council defines cyber-attack as "deliberate actions to alter, disrupt, deceive, degrade, or destroy computer systems or networks or the information and/or programs resident in or transiting these systems or networks." Although the objective-based definitional approach taken by the United States is pretty clear, the complexity of these definitions fails to distinguish between a simple cyber-crime and a cyber-attack.

The Shanghai Cooperation Organization—a security cooperation group composed of China, Russia, and most of the former Soviet Central Asian republics, as well as observers—has adopted a much more expansive means-based approach to cyber-attacks. The Organization has "express[ed] concern about the threats posed by possible use of [new information and communication] technologies and means for the purposes incompatible with ensuring international security and stability in both civil and military sphere". Also the New Strategic Concept does not consider automatically cyber attacks as a threat justifying the use of force by the Alliance. NATO art. 5 has a clear formulation, but what has to be considered is that an Art. 5 attack is decided on a case by case basis.

However, on the light of the above a definition of cyber attack could be:

A cyber-attack consists of any action taken to undermine the functions of a computer network for a political or national security purpose-

A cyber-attack's means can include *any* action—hacking, bombing, cutting, infecting, and so forth—but the objective can only be to undermine or disrupt the function of a computer network.

The objective of a cyber-attack must be to undermine the *function* of a computer network.

Mere cyber-espionage, or cyber-exploitation, does not constitute a cyber-attack, because neither of these concepts involves altering computer networks in a way that affects their current or future ability to function. To "undermine the function" of a computer system, an actor must *do more than passively observe a computer network or copying data*, even if that observation is clandestine.

Such activities may be criminal—as acts of corporate or political cyber-espionage—but are not cyber-*attacks*. In this respect, our definition reflects a common distinction between espionage and attacks in more traditional settings.

A political or national security purpose distinguishes cyber-attack from simple cyber-crime. Any aggressive action taken by a state actor in the cyber-domain necessarily implicates national security and is therefore a cyber-attack (where the action satisfies all the other elements of the definition), whether or not it rises to the level of cyber-warfare.

Not every cyber attack, therefore, constitutes an armed attack. According to some scholars, a cyber attack alone will almost never constitute an armed attack for the purposes of Art. 51 because it lacks the physical characteristics traditionally associated with military coercion, in other words because it generally makes no use of traditional military weapons.

This approach treats the cyber attack as an armed attack only if it uses military weapons. This instrument-based approach's chief advantage is the simplicity of application since use of military weapons and force are relatively easy to identify. However, because cyber attacks have the potential to cause catastrophic harm without employing traditional military weapons, most scholars have rejected the instrument-based approach to defining armed attack as dangerously outdated. On the contrary, the best test could be whether a cyber attack results in physical destruction –sometimes called a kinetic effect- comparable to a conventional attack. This effect-based approach classifies a cyber attack as an armed attack based on the gravity of its effects. The problem with the effect-based approach, however, lies in articulating ex ante what types of effects justify the self defence.

The most important instrument of international law in order to label actions take between states is the UN Charter. The Charter lists different levels of undesirable actions committed by states; use of force (article 2.4), threats to the peace, breach of the peace or act of aggression (article 39), and armed attack (article 51). as confirmed in the resolution on the aggression adopted by ICC Review Conference (Resolution RC/Res.6, 11 June 2010).

However, the Cyber attack is different from the traditional aggression. Cyber attacks lack the geospatial limitations of aggression. The Internet's structure permits attacks to occur from any part of the globe against any target with no early warning or indication. International attempts to regulate cyber attacks should create individual accountability for the malfeasance of State and non-State actors.

The Review Conference made an express reference to the 1974 GA Resolution considering "acts of aggression" the *"use of armed force by a State against the sovereignty, territorial integrity or political independence of another State or in any other manner inconsistent with the Charter of the United Nations*" as provided by art. 1 of 1974 GA Resolution, and including the list of acts provided from Article 3 of the same Resolution, but eliminating every reference to Article 4.
Under the definition provided at paragraph 1 of the amended Statute, the "crime of aggression" is, on the contrary, committed *"by a person in a position effectively to exercise control over or to direct the political or military action of a State"*. Thus, the crime is solely a "leadership crime" and this understanding is confirmed as well by the amendment to Rome Statute inserting into Article 25 a paragraph 3bis stating "In respect of the crime of aggression, the provisions of this article shall apply only to persons in a position effectively to exercise control over to direct the political or military action of a State".
This "leadership clause" referred to the "crime of aggression" limits culpable conduct to those with direct control over political or military action of the State, providing significant limitations on the regulation of cyber attacks, since the vast majority of cyber attacks are conducted by individuals with only tenuous affiliations to a collective.
Moreover, eliminating every reference to art. 4 of the 1974 GA Resolution from art. 8b of the Rome Statute, the SWGCA has severely restricted the application of their definition to cyber warfare. Yet cyber warfare certainly has the potential to create catastrophic damage well beyond that resulting from a threshold traditional weapons attack. The interpretation of the list as open could conceivably include cyber attacks resulting in physical damages, but may not include the significant threat of non-lethal communication and economic disruption through cyber tactics. The SWGCA definition also includes a *de minimis* clause, by limiting the definition to acts which, "by [their] character, gravity and scale, constitute manifest violation[s] of the Charter of the United Nations." The *de minimis* clause provides an important qualifier for the regulation of cyber attacks under the definition. Many cyber attacks do not rise to the level of activity to warrant involvement by the ICC. Furthermore, the *de minimis* clause makes clear only manifest violations of the UN Charter would trigger culpability under the statute.

ii) The second grey area is the problem of cyber attacks attribution, which is one of the most significant challenges to deterring attacks in cyberspace or lunching retaliatory attacks to the aggressor. The solution of that problem is a difficult but necessary task in order to strengthen cyber security.
The relevant ILC section regulating attribution states that "the conduct of any State organ shall be considered an act of that State under international law" and that an organ includes "any person or entity which has that status in accordance with the internal law of the State".
The current State actor requirement in international law greatly limits its applicability to cyber attacks as evidence certainly shows that most of the attacks on a State are carried out by individuals without affiliation to a State.
Under article 8 ILC "The conduct of a person or group of persons shall be considered an act of a State under international law if the person or group of persons is in fact acting on the instructions of, or under the direction or control of, that State in carrying out the conduct."
The current trend of international practice provides a broad interpretation of the meaning of control (ICTY, Tadic case), which is not strictly linked to the delivery of instructions, raising the possibility that private individuals can be considered as de facto State's organs.
This approach surpasses the "**effective control**" doctrine (ICJ, Nicaragua case) permitting to overreach the strict requirements expressed by the quoted art. 8 ILC and to dwell on the de facto parameters to establish the existence of a overall control, such as, for example, that one given by the logistic/technical support provided by the State.
Clearly even the compliance of the State, or the tolerance towards these groups of individuals, implies that the State does not respect the duties of due diligence over activities on its territory.

C. METHODOLOGY

C.1 LEGAL FRAMEWORK OF REFERENCE

The legal framework of reference is given by the rules of international law (customary law, treaties, law of armed conflicts, private international law rules), and by acts of international organizations (United Nations, ITU, NATO, European Union and OSCE.
(For the rules of customary law see B.2.1.)

C.1.1 EUROPEAN UNION APPROACH TO CYBERSECURITY

The European Union (EU)'s attention towards cyber threats has increased over time, in particular in the second half of the 2000s.

At the strategic level, EU documents have been increasingly dealing with cyber security and related threats, even though a clear-cut definition of their exact nature and contents is still missing.
The 2003 European Security Strategy (ESS) (not legally binding), EU's first-ever attempt to set out guidelines for an autonomous policy in the security domain, only mentions the general danger posed by the misuse of electronic networks. Yet two other documents adopted in 2008, the Council Statement on tighter international security and the Report on the Implementation of the European Security Strategy (both without binding force) explicitly mention cyber attacks and cyber security, perceived as growing threats to EU security. Under a complementary – intra EU – perspective, the 2010 EU Internal Security Strategy (not legally binding) focuses on cyber crime, generally understood as a "global, technical, cross-border, anonymous threat to (EU's) information systems". Further details on how to increase EU's resilience to cyber threats are included in the ensuing EU Internal Security Strategy in action (2010, not legally binding) that calls for improvement in three main areas: capacity building in law enforcement and judiciary; cooperation with private actors; reaction to cyber attacks and cyber disruptions and Commission has also developed, in 2011, within the European Forum for Member States (EFMS), a Communication on "Critical Information Infrastructure Protection 'Achievements and next steps: towards global cyber-security" to clarify what exploitation, disruption and destruction mean in refer to cyberspace.

Cyber initiatives carried out so far by the EU mainly falls within the cyber security domain (that is in a civilian domain) and aim at ensuring Network and Information Security (NIS). They include Critical Information Infrastructure Protection (CIIP), the fight against cyber crime, and, on the regulatory side, the framework for electronic communications (including data protection and privacy issues).
According to the 2006 Commission's Communication Strategy for a Secure Information Society (not legally binding), Network and Information Security is "the ability of a network or an information system to resist (…) accidental events or malicious actions that compromise the availability, authenticity, integrity and confidentiality of stored or transmitted data and the related services (…)" (p. 3). To this end, the protection of Critical Information Infrastructures (CIIs) is of outmost importance as it consists of all the activities of infrastructure owners and operators aimed at ensuring that in case of failures, attack or incidents the performance of critical information infrastructures is above a minimum level of services.

The EU is also particularly active in the fight against cyber crime, perceived as the threat with the most immediate impact on citizens' security and everyday lives. Nevertheless, efforts in this domain are hindered by the lack of a univocal definition of cyber crime across the EU. A Communication from the Commission of 2007 (not legally binding) sheds some light in this respect, identifying three main cyber crime categories: i) traditional forms of crime such as fraud and forgery, although in a cyber context; ii) the publication of illegal content over electronic media; iii) crimes unique to electronic networks, namely cyber attacks against information system, denial of service and hacking. Some more detailed examples of cyber attacks are contained in a 2005 EU Council Framework Decision (legally binding), which however does not distinguish between small- and large-scale cyber attacks and does not focus explicitly on attacks against CIIs. One hopes that such current gaps will be filled in the forthcoming reform of the Framework Decision. Helpful to harmonize cyber crime definitions can also be the Lisbon Treaty, which contains specific provisions for harmonization as regards computer crime (art. 83).

As it emerges from the main strategic and policy documents mentioned so far and from the 2010 European Digital Agenda' (not legally binding), the two priorities to improve EU's resilience and response to cyber attacks are, on the one hand, enhancing the awareness of the main risks related to cyber security and, on the other – operational – hand, increasing national and EU preparedness to cyber attacks and/or incidents.
At the operational level, national and EU efforts currently aim at creating or enhancing Computer Emergency Response Teams (CERTs), groups of experts gathering public and private actors that provide immediate assistance in the event of a cyber incident and conduct prevention, monitoring and training initiatives. A network of all national CERTs and the CERTs of European institutions is to be established by 2012 in order to gradually create an EU-centric governance of CERTs under ENISA's responsibility. As a first step towards an EU-CERT, a pre-configuration team has been recently set up and started operations on 1st June 2011.
Besides, crucial to improve national and EU' s preparedness and response to cyber attacks or incidents and to assess available capabilities are joint exercises. The first pan-European exercise, Cyber Europe 2010, involved all 27 Member States and 3 EFTA countries (Norway, Switzerland and Iceland), whose experts had to respond to 300 simulated hacking attacks aimed at paralyzing the Internet and critical online services across Europe. Unsurprisingly, the main conclusions driven from the exercise were that common procedures to handle cyber incidents do not yet exist at pan-European level and that there is a need to improve response collaboration across Europe. The next European exercise has been planned for 2012. In the meanwhile has been held the first EU-US cyber security exercise, Cyber Atlantic 2011, on November 2011.

C.2 CRITERIA AND RULES

The concept framework we suggest is patterned basically on a “rule oriented approach” rather than on a “policy oriented approach”, that is to say we take into consideration essentially the existing international law rules (customary law, treaties, soft law). These rules are apparently not directed to cyberspace, nevertheless they can provide answers to questions raised in this new context, if interpreted, as we do, by using the methodological tools coming from the general theory of law applicable to international law (i.e. analogy etc.), as well as interpretation rules of the Vienna Convention on the law of treaties.

C.3 ANALYTICAL MODEL

Introduction

The aim of MNE7 objective 3.3 is to improve partners and coalition members understanding of the current legal frameworks applicable to the cyber common, in order to handle cyber incidents, while providing decision-makers with appropriate tools that support decision options for response.

The Guidelines for Decision Makers for Cyber Incidents Handling (GDMs) are envisaged as the MNE7 Obj. 3.3 solution to provide the decision makers, mainly at the political and the strategic level, with a practical instrument to pin down, in a coherent framework, the main elements and features of a given cyber incident, support the analysis conducted by legal experts under a legal perspective and identify the appropriate options for a response.

Cyber Incident Analytical Model

The core idea under the GDMs is represented by the Cyber Incident Analytical Model depicted in the matrix at page 14, which offers a framework for the conduct of the legal analysis.

It is important to underline that the matrix, although long-discussed and shared among obj. 3.3 community, might be further developed and emended, as required in order to fill gaps eventually emerging along the progress of the concept & solution development phase of the MNE7 Objective 3.3 campaign.

The matrix highlights seven **main columns** (in green), designed for directing the legal analysis towards the key elements of a cyber incident to be taken into account under a legal perspective:

1. Context
   Intended as the status of the international relationships among the relevant actors involved in the cyber incident (peacetime, crisis, armed conflict, etc.). It is recognized that there will almost certainly be a blurring across all these categories in the future, as we face becoming involved in increasingly complex and wicked problems.

2. Actor
   International Law mainly applies to states and state actors, while a cyber incident may originate also within other organizations, entities or individuals whose responsibility under international law, or even the attribution of it, represent one the key elements to be investigated and carefully analysed in order to address appropriate responses under the international legal framework.

3. Assessment of activities
   The way information in the cyberspace is used, manipulated, influenced or exploited in order to determine desired or unintentional effects, by carrying out cyber attacks, cyber exploitation or, in the events with absence of an intentional will to produce consequences/damages, cyber defence. The intention, even though its relevance in the International Law perspective is questioned, could be evaluated in this assessment

4. Source
   In a legal analysis carried out across the International Law perspective, it could be decisive for an effective effort to identify appropriately which is the source a cyber incident may originate from (government, military, private).

5. Target/Objectives
   The target/objectives of a cyber incident may be located in the layers of state, military or private domain; among these elements, possible consequences affecting critical infrastructures and civilian infrastructures are of particular relevance, due for example to vital threats to a population security deriving from significant damages caused to them by a cyber incident.

6. Consequences
   The consequences resulting from a cyber incident, similarly to other categories of incidents, could result in casualties (human losses), physical damage, non material effects (e.g. psychological impact), economic et al, or, especially in the military field, it may affect Operational Security (OPSEC).

7. Extent
   The extent of consequences from a cyber incident might be scientifically unverifiable, but the perceived level of the extent could be a relevant factor in an (international legal) analysis aimed to provide assessments regarding legal options for response.

Within the analytical model framework, a given cyber incident can be described by highlighting the characterizing seven key elements in the appropriate boxes along every column.
More than one box may be highlighted, in each column, to describe the simultaneous presence of multiple features of the same element (e.g. a cyber attack carried out through privately owned nodes and public nodes at the same time, or effects on multiple systems of a state).
Subsequently, the legal analysis of the given cyber incident may be conducted, column by column, by relating each element (column) and feature (highlighted boxes) to the notions of the international legal framework which apply.
The final outcome of legal analysis should be highlighted through the elements in the last two columns (in blue). In fact, the identified breach of an international obligation, as a result from the guided analysis across the eight green columns, shall drive to the assessment of the related legal threshold. Should the cyber incident be identified as a domestic issue (Internal), Response Options will have to be selected within the applicable Domestic Legal Frameworks; in all other cases (wrongful act, international crime, armed attack) possible response options (among those available depending on the Decision Maker's own level of authority) will also have to be assessed against the International legal framework.
It is important to underline that the mutual influence among the elements of the analytical model as well as the possible interactions among relevant features shall also be taken into account to **avoid any mechanistic approach to the legal analysis**.

Analytical model matrix

Context	Actor	Assessment of activities	Source	Target/ Objectives	Consequences	Extent	Breach of an international obligation	Legal Thresholds	
Peace time	State	Cyber Attack - disruptive - destructive	State	State	Non material	Small		Domestic Issue	
Crisis	Person/Entity	Cyber Defence	Military	Military	Economic	Mild	Sovereignty. Non interference on internal affairs of a State. Human rights: Freedom of Expression	Wrongful Act	
Armed Conflict	Terrorist	Cyber Exploitation	Private	Private	Physical Damage	Large	Prohibition of use of force and threat. Humanitarian law	International Crime	Terrorism
	Undetermined	Undetermined	Undetermined	Critical Infrastructure	OPSEC				Crime of Aggression
				Civilian Infrastructure	Casualties			Armed Attack	

Example of Response Matrix

Thresholds		Options for Response			
Domestic Issue		Internal Response Options based on Domestic Legal Frameworks			
Wrongful Act		Gain support through the United Nations.	Alert and introduce special teams (e.g., public diplomacy).	Identify the steps to peaceful resolution.	Take actions to gain support of allies and friends.
		Increase cultural group pressure.	Reduce international diplomatic ties.	Reduce security assistance programs.	Ensure consistency of strategic communication messages.
		Enact restrictions on technology transfer.	Enact restrictions on technology transfer.	Encourage national and international financial institutions to restrict or terminate financial transactions.	Encourage national and international financial institutions to restrict or terminate financial transactions.
		Protect friendly communications systems and ISR assets (computer network defence, operations security, information assurance).	Publicize violations of international law.	Maintain an open dialogue with the news media.	Take steps to increase national public support.
		Freeze or seize real property where possible.	Freeze or seize real property where possible.	Freeze or seize real property where possible.	
		Make public declarations of non-proliferation policy.	Impose sanctions on communications systems and intelligence, surveillance, and reconnaissance (ISR) technology transfer.	Initiate non-combatant evacuation procedures.	Increase informational efforts:
		Increase communication systems and ISR processing and transmission capability.	Restrict activities of diplomatic missions.	Prepare to withdraw or withdraw embassy personnel.	Embargo goods and services.
		Increase defence support to public diplomacy.	Increase information operations.	Demonstrate international resolve.	Enact trade sanctions.
International Crime	Terrorism	Publicize increased force presence, joint exercises, military capability.	Upgrade alert status.	Restrict travel of national citizens.	Increase intelligence, surveillance, and reconnaissance.
		Influence adversary decision makers (political, military, and social).	Increase training and exercise activities.	Initiate or increase show-of-force actions.	Increase active and passive protection measures.
		Implement meaconing, interference, jamming, and intrusion of adversary informational assets.	Increase information measures directed at the opponent's military forces.		
	Crime of Aggression	Interrupt satellite downlink transmissions.	Deploy forces into or near the potential operational area.	Rapid Response	Limited Response
Armed Attack		Decisive Response			

Source: JP-5 August 2011, Appendixes E and F.

D. SOLUTIONS

D.1 Guidelines for Decision Makers – Legal Analysis for Cyber Incidents (GDMs)

The GDMs are considered the main Obj. 3.3 product, describing the process for conducting the legal analysis of a given cyber incident.

The aim of the GDMs is to provide legal advisors and SMEs with a supporting tool for identifying the legal threshold crossed by a cyber incident in terms of violation of the international law and recommend lawful options for response to the decision makers of the political/strategic/high operational level. In this regard, it has been argued that the audience for GDMs as a product may be identified as the legal advisors/SMEs rather than the decision makers themselves. In this case, the denomination of the product should be redefined accordingly.

GDMs are not expected at all to be run as a mechanistic tool that produces univocal outputs on the base of juridically qualified inputs, making unnecessary the sensible role and function to be played by legal experts. Nevertheless, GDMs are aimed to support the legal assessment process framing it within a legally coherent perspective.

Furthermore, the value of the product in itself has been questioned during the debate, arguing that legal advisors are usually able to conduct their legal analysis processes without the need of supporting tools. While it has been clarified that the GDMs are not intended as a mechanistic approach to the legal analysis, nor an imperative source on how to inform the legal analysis of events occurring in the cyber common, the above mentioned concern was reputed as a decision point for further development of the obj. 3.3 CD&E campaign and will be considered as the main experiment issue for the LOE, where the added value of the GDMs as a supporting tool for conducting cyber legal analysis will be measured and scrutinized.

D.2 Cyber Incident Vignettes (CIVs)

The CIVs are a set of situations describing cyber incidents. The main purpose of CIVs is to validate the GDMs through a campaign of experimentation aimed at testing their soundness (unambiguousness of interpretation) as a supporting tool for legal analysis of cyber incidents and their ability of improving the efficiency of the analysis process.

To this end, obj. 3.3 contributing nations provided an initial set of 59 vignettes, which has been published on the MNE7 Portal. The level of detail of those vignettes spans from very generic to exceedingly detailed for the purposes of legal analysis. Also the range of diverse situations described probably does not fit the requirements for GDMs development and experimentation. Therefore, Obj. 3.3 contributing nations agreed on the opportunity of identifying a common standard for the description of the vignettes, according to the key elements of a cyber incident defined in the analytical model. Taking into consideration CD&E requirements and an inter-domain focus, ITA will recognize the current collection of CIVs selecting a subset of growing complexity situations, and subsequently ask the contributing nations to provide a new draft according to the agreed standard.

Considerations on the feasibility of the LOE suggest that the final number of CIVs resulting from the experimentation will not exceed 12 vignettes analysed and commented by legal experts. The question of considering so small an amount of final commented CIVs as a reference product for legal analysis is under scrutiny.

D.3 Study Report on Sovereignty and Jurisdiction (SR)

The Study Report “Influence of Information Technology Developments on the Traditional Legal Concepts of Sovereignty and Jurisdiction” addresses the broad topic of how contemporary IT practices, such as the sharing of personal data in e-commerce activities, transition to cloud-based services and efforts to tackle cyber crime, align with the notions of sovereignty and jurisdiction. The Study Report first gives a theoretical overview of these legal concepts, and then, based on a few real-world examples, puts them into the context of today’s information society. Due to its novel problem statement and a variety of practical examples, the Study Report provides interesting reading to lawyers as well as other professionals acting in the field of cyber security. The Study Report is primarily meant to raise awareness and encourage discussion on a topic that is of a very legal nature, but the implications of which influence private companies, end-users, investigators, and others.

The Study Report is developed by NATO CCD CoE and will be an additional product along obj.3.3 development.

D.4 Cyber Legal Lexicon (CLL)

The Cyber Legal Lexicon CLL is aimed at collecting terms and definitions coming from diverse sources, including international law, in order to reach a common understanding of the terminology already applied or applicable to the cyber common. The development of CLL is led by the CCD CoE.

Three main categories of terms have been identified so far for the purposes of obj. 3.3:

- widely accepted (even though with different interpretations and nuances) terms and expressions deriving from policy, doctrine and technical sources (i.e. cyberspace, cyber defence, cyber attack, cyber threats, cyber crime, etc.). Most of these terms have been proposed by the CCD CoE for inclusion in the early version of the MNE7 lexicon and acknowledged on a consent basis from the outcome custodians. These terms will be directly incorporated in the CLL and synchronized with the MNE7 lexicon where beneficial;
- terms and expressions attaining the juridical dimension of the cyberspace, whose definitions, directly flowing from the international law, are quite stringent (i.e. wrongful act, international crime, act of aggression, armed attack, etc.). These terms, where employed within obj. 3.3 products, will be included in the CLL;
- working terminology of new coinage, deemed useful by obj. 3.3 concept developers and endorsed by SMEs (i.e. armed attack through cyber means, cyber legal analysis, etc.). These terms and expressions, will be staffed among obj. 3.3 contributing nations and included in the CLL on a consent basis.